

Presented to the Court by the foreman of the
Grand Jury in open Court, in the presence of
the Grand Jury and FILED in the U.S.
DISTRICT COURT at Seattle, Washington.

August 28 2019
WILLIAM M. McCOOL, Clerk
By [Signature] Deputy

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff

v.

PAIGE A. THOMPSON,

Defendant.

CR19-159 RSL
INDICTMENT

The Grand Jury charges that:

COUNT 1
(Wire Fraud)

1. Beginning in or before March 2019, and continuing until in or after July 2019, at Seattle, within the Western District of Washington, and elsewhere, PAIGE A. THOMPSON, with the intent to defraud, devised and intended to devise, a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises.

A. *Background*

2. The "Cloud Computing Company" is a company that provides cloud-computing services to individuals, companies, and governments. Cloud computing is the practice of using a network of remote servers hosted on the Internet, commonly referred to as "the cloud," rather than a local computer or server, to store, manage, and process

1 data. The Cloud Computing Company provides services through server farms that are
2 located throughout the world and maintained by the Cloud Computing Company.

3 3. Capital One Financial Corporation (“Capital One”) is a bank holding
4 company that offers credit cards and other services to customers throughout the United
5 States. Capital One supports its services, in part, by renting or contracting for computer
6 servers from the Cloud Computing Company. The servers on which Capital One stores
7 credit card application and other information generally are located in states other than the
8 State of Washington, and they store information regarding customers, and support
9 services, in multiple states. Deposits of Capital One are insured by the Federal Deposit
10 Insurance Corporation.

11 4. Victim 2 is state agency of a state that is not the State of Washington.
12 Victim 2 supports its services, in part, by renting or contracting for computer servers
13 from the Cloud Computing Company.

14 5. Victim 3 is a telecommunications conglomerate located outside the United
15 States that provides services predominantly to customers in Europe, Asia, Africa, and
16 Oceania. Victim 3 supports its services, in part, by renting or contracting for computer
17 servers from the Cloud Computing Company.

18 6. Victim 4 is a public research university located outside the State of
19 Washington. Victim 4 supports its services, in part, by renting or contracting for
20 computer servers from the Cloud Computing Company.

21 *B. The Essence of the Scheme and Artifice*

22 7. The object of the scheme was to exploit the fact that certain customers of
23 the Cloud Computing Company had misconfigured web application firewalls on the
24 servers that they rented or contracted from the Cloud Computing Company. The object
25 was to use that misconfiguration in order to obtain credentials for accounts of those
26 customers that had permission to view and copy data stored by the customers on their
27 Cloud Computing Company servers. The object then was to use those stolen credentials
28 in order to access and copy other data stored by the customers on their Cloud Computing

1 Company servers, including data containing valuable personal identifying information.
2 The object also was to use the access to the customers' servers in other ways for PAIGE
3 A. THOMPSON's own benefit, including by using those servers for "cryptojacking."

4 C. *The Manner and Means of the Scheme and Artifice*

5 8. It was part of the scheme and artifice that PAIGE A. THOMPSON used,
6 and created, scanners that allowed her to scan the publicly facing portion of servers
7 rented or contracted by customers from the Cloud Computing Company, and to identify
8 servers for which web application firewall misconfigurations permitted commands sent
9 from outside the servers to reach and be executed by the servers.

10 9. It was further part of the scheme and artifice that PAIGE A. THOMPSON
11 then transmitted commands to the misconfigured servers that obtained the security
12 credentials for particular accounts or roles belonging to the customers with the
13 misconfigured servers.

14 10. It was further part of the scheme and artifice that PAIGE A. THOMPSON
15 then used the accounts for which she had obtained security credentials to obtain lists or
16 directories of folders or buckets of data in the Cloud Computing Company customers'
17 storage space at the Cloud Computing Company.

18 11. It was further part of the scheme and artifice that PAIGE A. THOMPSON
19 used the accounts for which she had obtained security credentials to copy data, from
20 folders or buckets of data in the Cloud Computing Company customers' storage space at
21 the Cloud Computing Company for which the accounts had requisite permissions, to a
22 server that PAIGE A. THOMPSON maintained at her own residence.

23 12. It was further part of the scheme and artifice that, in taking these steps,
24 PAIGE A. THOMPSON implicitly represented that commands to copy data that she sent
25 using the accounts for which she had obtained security credentials were legitimate
26 commands sent by users with permission to send such commands, rather than commands
27 sent by a person who had stolen the security credentials and who lacked authority to use
28 the accounts and send the commands.

1 13. It was further part of the scheme and artifice that, in executing the scheme
2 and artifice, PAIGE A. THOMPSON used virtual private networks (“VPNs”), including a
3 VPN offered by the company IPredator, to conceal PAIGE A. THOMPSON’s location
4 and identity from the Cloud Computing Company and from victim companies.

5 14. It was further part of the scheme and artifice that, in executing the scheme
6 and artifice, PAIGE A. THOMPSON used The Onion Router (“TOR”) to conceal PAIGE
7 A. THOMPSON’s location and identity from the Cloud Computing Company and from
8 victim companies.

9 15. It was further part of the scheme and artifice that PAIGE A. THOMPSON
10 copied data to her own server from servers rented or contracted by Capital One from the
11 Cloud Computing Company, including data that contained information, including
12 personal identifying information, from approximately 100,000,000 customers who had
13 applied for credit cards from Capital One.

14 16. It was further part of the scheme and artifice that PAIGE A. THOMPSON
15 copied and stole data from more than 30 different entities, including Capital One,
16 Victim 2, Victim 3, and Victim 4 that had contracted or rented servers from the Cloud
17 Computing Company.

18 17. It was further part of the scheme and artifice that PAIGE A. THOMPSON
19 used her unauthorized access to certain victim servers – and the stolen computing power
20 of those servers – to “mine” cryptocurrency for her own benefit, a practice often referred
21 to as “cryptojacking.” (Cryptocurrency mining is the process by which cryptocurrency
22 transactions are verified and added to the public ledger, *i.e.*, the blockchain. Persons who
23 verify blocks of legitimate transactions, often referred to as “miners,” are rewarded with
24 an amount of that cryptocurrency. Successful mining operations consume large amounts
25 of computing power and hardware.)

26 C. *Execution*

27 18. On or about March 22, 2019, at Seattle, in the Western District of
28 Washington, and elsewhere, PAIGE A. THOMPSON, for the purpose of executing the

1 scheme and artifice described above, caused to be transmitted by means of wire
 2 communication in interstate commerce, from her computer in Seattle to a computer
 3 outside the State of Washington, writings, signs, signals, pictures, and sounds, that is, a
 4 command to copy data belonging to Capital One from servers, rented or contracted by
 5 Capital One from the Cloud Computing Company, to a server belonging to PAIGE A.
 6 THOMPSON in Seattle.

7 All in violation of Title 18, United States Code, Section 1343.

8
 9
 10 **COUNT 2**
(Computer Fraud and Abuse)

11 19. The allegations set forth in Paragraphs 1-18 of this Indictment are realleged
 12 and incorporated into this Count, as if fully set forth herein.

13 20. Between on or about March 12, 2019, and on or about July 17, 2019, at
 14 Seattle, within the Western District of Washington, and elsewhere, PAIGE A.
 15 THOMPSON intentionally accessed a computer without authorization, to wit, a computer
 16 containing information belonging to Capital One Financial Corporation, and thereby
 17 obtained information contained in a financial record of a financial institution and of a
 18 card issuer as defined in Section 1602 of Title 15, and information from a protected
 19 computer, and the value of the information obtained exceeded \$5,000.

20 All in violation of Title 18, United States Code, Section 1030(a)(2)(A) and (C),
 21 and (c)(2)(A) and (B)(iii).

22
 23 **ASSET FORFEITURE ALLEGATION**

24 **(Count 1)**

25 The allegations contained in Count 1 of this Indictment are hereby realleged and
 26 incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18,
 27 United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section
 28 2461(c). Upon conviction of the offense charged in Count 1, the defendant, PAIGE A.

1 THOMPSON, shall forfeit to the United States any property, real or personal, which
 2 constitutes or is derived from proceeds traceable to such offense, including but not
 3 limited to a judgment for a sum of money representing the property described in this
 4 paragraph.

5 **(Count 2)**

6 The allegations contained in Count 2 of this Indictment are hereby realleged and
 7 incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18,
 8 United States Code, Sections 982(a)(2)(B) and 1030(i). Upon conviction of the offense
 9 charged in Count 2, the defendant, PAIGE A. THOMPSON, shall forfeit to the United
 10 States any property constituting, or derived from, proceeds the defendant obtained,
 11 directly or indirectly, as the result of such offense, and shall also forfeit the defendant's
 12 interest in any personal property that was used or intended to be used to commit or to
 13 facilitate the commission of such offense, including but not limited to a judgment for a
 14 sum of money representing the property described in this paragraph.

15 **(Substitute Assets)**

16 If any of the above-described forfeitable property, as a result of any act or
 17 omission of the defendant,

- 18 a. cannot be located upon the exercise of due diligence;
- 19 b. has been transferred or sold to, or deposited with, a third party;
- 20 c. has been placed beyond the jurisdiction of the Court;
- 21 d. has been substantially diminished in value; or
- 22 e. has been commingled with other property which cannot be divided without
- 23 difficulty;

1 it is the intent of the United States, pursuant to Title 18, United States Code, Sections
2 982(b) and 1030(i)(2), Title 21, United States Code, Section 853(p), and Title 28, United
3 States Code, Section 2461(c), to seek the forfeiture of any other property of the
4 defendant, up to the value of the above-described forfeitable property.
5

6 A TRUE BILL:

7 DATED: August 26, 2019

8 *Signature of foreperson redacted*
9 *pursuant to the policy of the Judicial*
10 *Conference of the United States*

11 FOREPERSON

12
13 

14 BRIAN T. MORAN
15 United States Attorney

16
17 

18 ANDREW C. FRIEDMAN
19 Assistant United States Attorney

20
21 

22 STEVEN T. MASADA
23 Assistant United States Attorney
24
25
26
27
28